

PCI-nyhedsbrev – august 2010

Indhold:

1. Amerikansk PCI-lov indvarsler nye tider i Europa
2. Chipkortet på vej til at ændre PCI-standarden
3. Ny standard for PCI-scanninger ændrer processen
4. De simple PCI-løsninger er tit bedst og billigst

1. Amerikansk PCI-lov indvarsler nye tider i Europa

I dag er der ingen specifik lovgivning på PCI-området i Danmark. Vi har kun PCI-standarden, som ikke er en lov, men en frivillig aftale mellem to parter, som er underkastet de almindelige aftaleretlige regler. Sådan har det hidtil også været i USA, men her er der nu lovregler om kreditkortsikkerhed på vej, og den tendens vil formentlig også brede sig til EU og Danmark i fremtiden. Blandt andet er der med sikkerhed lovregler om datalækage på vej i Europa.

De amerikanske regler

De nye amerikanske lovregler betyder, at man nu har valgt at inkludere regler om beskyttelse af kreditkort i lovgivningen i Nevada, Minnesota og senest Washington, og det er sandsynligt, at flere stater vil følge trop.

Den nyeste lov i Washington trådte i kraft 1. juli 2010 og medfører, at amerikanske virksomheder nu er tvunget til at overholde bestemte regler på kreditkortområdet. Formålet med loven er, at en udstederbank skal have mulighed for at få kompensation for udgifter til udstedelse af nye kort, hvis en butik med mere end 6 mio. transaktioner eller kortprocesser mister kortdata, fordi dataene ikke var ordentligt beskyttet. I Nevada har man i stedet valgt gennem lovgivningen at kræve, at erhvervslivet skal overholde PCI-standarden.

Hvad kommer det til at betyde for EU?

I EU er der naturligvis stor interesse for, om der ligesom i USA vil blive indarbejdet PCI-lignende krav på nationalt eller europæisk niveau. Står det til kreditkortselskaberne, ser man helst, at der ikke indføres lovgivning. Her foretrækker man, at man selv kan formulere og styre reglerne. Og for tiden er der da heller ikke tegn på, at vi får lovgivning om beskyttelse af kreditkort foreløbig. Omvendt har Europa generelt haft tradition for at bygge forbrugerbeskyttelse ind i lovgivningen, og derfor vil vi alligevel i en nær fremtid se flere nye love, som berører betalingssikkerhed, i EU-regi.

I forbindelse med SEPA-direktivet, der primært vil blive implementeret i Euro-landene, vil der eksempelvis blive indført et krav om, at betalinger skal ske med chipkort, allerede i år. Desværre siger EU-reglerne intet om, hvilke sanktioner der vil være, hvis kravet om chipbetaling ikke efterleves.

Regler om datalækage på vej i EU

Når det gælder forbrugerbeskyttelse i forbindelse med datalækage, har man allerede i dag lovregler på området i USA. Reglerne betyder, at hvis man mister data, så har man pligt til at stå offentligt frem og redegøre for datatabet.

Lignende regler er også på vej ind i EU-lovgivningen, og Storbritannien har eksempelvis allerede nu indført sanktionsmuligheder i forbindelse med databas i lovgivningen.

Siden 6. april i år har Information Commissioner's Office (ICO) fået bemyndigelse til at udskrive bøder og give påbud ved databas. Bøderne kan i dag være på op til 500.000 pund i modsætning til før 6. april, hvor de var på maksimalt 6.000 pund. Reglerne blev indført efter en skandale, hvor toldmyndighederne mistede oplysninger om 25 mio. briter, fordi oplysninger lå på en cd, som gik tabt i posten.

Marks & Spencer fik eksempelvis også et påbud om at kryptere alle deres bærbare computere, efter at de havde mistet oplysninger om 26.000 ansatte, fordi en medarbejder fik stjålet sin computer.

I modsætning til de amerikanske regler kræver de britiske regler dog ikke, at man skal offentliggøre alle hændelser om databas.

På EU-plan er den såkaldte Digital Agenda også på vej. Den har syv hovedinitiativer, som betyder, at der snart vil blive indført regler om, at internetudbydere skal offentliggøre hændelser, hvor de taber personfølsomme data. Reglerne vil formentlig senere blive bredt ud, så de kommer til at omfatte andre typer af virksomheder.

Reglerne vil styrke kreditkortsikkerheden i EU og Danmark

I forhold til kreditkortsikkerheden i EU og Danmark er det FortConsults vurdering, at de kommende EU-lovregler vil være en klar styrkelse.

For det første vil det gavne både virksomheder og forbrugere, fordi vi får øget gennemsigtigheden, når vi begynder at få mere information om omfanget af databas i Europa, hvis virksomhederne i højere grad tvinges til at stå frem. Det vil gøre det langt tydeligere for virksomhederne, hvorfor det er så vigtigt at have styr på kreditkortsikkerheden.

Samtidig vil reglerne skabe et langt mere håndgribeligt incitament blandt virksomhederne til at beskytte dataene bedst muligt, fordi det vil skade deres omdømme, hvis et databas tvinger dem til at stå offentligt frem, og de samtidig risikerer økonomiske sanktioner.

2. Chipkortet på vej til at ændre PCI-standarden

Chipkortet er så småt ved at erstatte kort med magnetstribe i USA, og det er samtidig PCI Councils intention, at PCI-standarden skal tilpasses chipkort. Det er godt nyt for Danmark og resten af Europa, hvor man længe har efterlyst en ændring af PCI-standarden, fordi chipkortet her er langt mere udbredt end kort med magnetstribe.

PCI-standarden tager udgangspunkt i kort med magnetstribe

PCI-standarden, som vi bruger i Europa, herunder Danmark, er som bekendt fra USA. Derfor tager standarden også udgangspunkt i, at den skal beskytte kreditkort med magnetstribe, fordi det stadig er den korttype, der er langt mest udbredt i USA.

PCI-standarden har uden tvivl sin berettigelse pga. det store antal kortnumre, der bliver kopieret og misbrugt over hele verden. I flere årtier har det været muligt at kopiere en magnetstribe fra et kort og derefter lægge indholdet ned på et andet kort. Det er dog først inden for de seneste fem-ti år, at de kriminelle for alvor har fået fokus på svindel vha. teknologi og internettet, fordi alle betalingssystemer nu direkte eller indirekte er forbundet til internettet. PCI Council har derfor siden 2004 fokuseret på at udvikle PCI-standarden, så kortnumrene bliver beskyttet under opbevaring og ved betaling.

Chipkortet er et skridt tættere på sikker teknologi

I Danmark og resten af Europa er vi imidlertid overvejende gået væk fra kreditkort med magnetstribe og over til de langt mere sikre chipkort (EMV). Men fordi vi bruger den samme PCI-standard som USA, skal vi alligevel overholde de samme 240 sikkerhedspunkter som amerikanske virksomheder, fordi reglerne ikke tager højde for, at de europæiske kort er langt mere sikre.

Det betyder, at PCI-standarden reelt ikke matcher de europæiske forhold, som det er i dag, fordi den ikke tager højde for den højere sikkerhed i chipkort.

For mens PCI-standarden i virkeligheden er designet til at skabe sikkerhed omkring en usikker teknologi – nemlig kreditkort med magnetstribe – har vi i Europa valgt at gå i retning af, at vi i stedet hellere vil have en teknologi, som grundlæggende er sikker, i form af chipkort.

Konsekvensen er, at mange af de kontroller, der er i PCI-standarden i dag, bliver mindre vigtige i Europa, set ud fra et sikkerhedssynspunkt. De bliver dermed reduceret til en slags compliance-tjek.

Derfor har der fra mange fronter længe været et ønske om, at USA skal indføre EMV-kort, så de kan højne sikkerhedsniveauet, og så PCI-standarden samtidig kan blive moderniseret og komme til at matche det europæiske sikkerhedsniveau.

Fordelene ved EMV

Fordelen ved EMV er helt overordnet, at det indeholder en lille computer, som er involveret i selve transaktionen. Kortet indeholder et digitalt id, som kortet bruger til at bevise sin autenticitet som en del af transaktionen. I de nyere kort er sikkerheden forbedret ved at bruge Dynamic Data Authentication (DDA), som tilføjer en "random challenge/response" til autorisationsprocessen.

Processen foregår ved, at terminalen sender transaktionsinformation og et tilfældigt tal til chipkortet. Chippen bruger en intern privat nøgle til at generere en unik digital signatur til den specifikke transaktion. Chippens transaktionssignatur bliver tjekket vha. en offentlig nøgle af terminalen og netværket som en del af autorisationsprocessen. Det er kun en uforfalsket chip, der kan levere en gyldig signatur på grundlag af de data, den får, og derfor bekræfter DDA-processen, at kortet er både ægte og til stede. Det er chippen i kortet, der beregner responsen internt, så de vigtige informationer forlader ikke chippen, og derfor kan informationerne ikke bare kopieres, som det er tilfældet med et kort med magnetstribe.

EMV har igennem mange år været et robust værn imod angreb, og teknologien anses stadig for at være relativt sikker i dag. I europæisk perspektiv er det dog et problem, at vores kort stadig skal være udstyret med magnetstribe, så de også kan bruges uden for EU. Magnetstriben kan nemlig kopieres og bruges til at lave kortkopier, der kan misbruges i udlandet. Det betyder bl.a., at PCI-reglerne tvinger en stor udgift ned over mange virksomheder, fordi der på den måde sker korttyverier fra de usikre magnetstribesystemer (og gennem e-handel).

FortConsult har udført mange audits gennem de seneste seks år. Hovedparten har fundet sted i Europa, men vi har også lavet en del i USA, Kina, Rusland, Canada og flere andre steder uden for Europa. Vores erfaring viser klart, at EMV markant begrænser muligheden for at stjæle data.

Derfor ser vi meget positivt på, at der i USA er tegn på, at man ønsker at benytte EMV, og at det PCI Councils intention, at de i den kommende version af PCI-standarden vil prøve at tilpasse reglerne til chipkortet – selvom vi endnu ikke ved hvordan. Det vil nemlig gavne både de danske og de øvrige virksomheder, der har implementeret EMV, fordi man med chipkortet tager fat ved problemets rod: at magnettribeteknologien grundlæggende er for usikker.

WalMart vælger chipkortet

I USA har bl.a. supermarkedskæden WalMart for nylig indført betaling med chipkort og pinkode for at øge sikkerheden. Al WalMarts hardware er allerede klar til at benytte EMV-teknologien, og de arbejder i øjeblikket på at færdiggøre softwaren.

Ellen Richey, chief enterprise risk officer hos Visa, USA, har bl.a. kommenteret problemstillingen i USA. I den forbindelse sagde hun, at det ikke er et spørgsmål om, hvorvidt USA skal eller ikke skal gå over til chip, men i stedet et spørgsmål om hvornår og hvordan. Samtidig har Richey sagt, at Visa mener, at chipteknologien øger sikkerheden og gør det både nemmere og hurtigere at handle for både kunder og virksomheder, og at Visa derfor støtter teknologien 100 pct.

Der er dog stadig lang vej endnu, før chipkortet er den dominerende kreditkorttype i USA, men efterhånden som det vinder indpas, er håbet, at PCI-standarden også vil blive tilpasset den nye og mere sikre virkelighed i USA og dermed også Europa.

Chipkortet løser imidlertid ikke problemet med sikkerheden, når det gælder onlinebetaling, hvor man stadig bruger kortnummeret, udløbsdatoen og evt. kontrolcifrene. Så på det område vil der stadig være de samme udfordringer med at skabe sikkerhed omkring oplysningerne, men også her bliver der arbejdet på nye og mere sikre løsninger – men det ligger noget længere ude i fremtiden.

3. Ny standard for PCI-scanninger ændrer processen

Jeres ASV (Approved Scanning Vendor) vil fremover begynde at stille nogle andre spørgsmål og gøre nogle andre ting, end I er vant til, når I skal have lavet PCI-scanninger. Det skyldes, at PCI Council har ændret reglerne i den del af PCI-standarden, som har med scanning at gøre. Det stiller nye krav til ASV'ernes ydelser.

ASV'en skal involveres mere i processen

De nye regler ændrer ikke voldsomt meget på typen af scanning. Der er stadig tale om en scanning, der overordnet set skal afsløre sårbarheder med nogen fokus på webapplikationer, men processen omkring scanningen er blevet grundlæggende ændret.

Selvom det hele tiden har været hensigten med PCI-scanningsreglerne, at ASV'en skal hjælpe kunden med scanningen, har de hidtidige regler reelt gjort det muligt, at en virksomhed selv kan stå for hele processen omkring en ASV-scanning. Det har betydet, at en ASV i virkeligheden blot har kunnet nøjes med at stille et webinterface til rådighed for sine kunder, som så via selvbetjening har kunnet indtaste informationer og IP-adresser og køre scanningen på egen hånd.

Problemet med den fremgangsmåde er, at en del PCI-scanninger er blevet udført forkert, fordi ASV'en ikke har kontrolleret, at de informationer, kunden indtaster i webinterfacet, også er de korrekte og nødvendige informationer. Den gamle løsning har dermed givet mulighed for betjeningsfejl, fordi ASV'erne i mange tilfælde har fortalt deres kunder, at en scanning kan klares med ganske få klik i et webinterface og intet andet. Dermed er der i princippet ingen garanti for, at virksomheden reelt er sikker, selvom den på papiret består PCI-scanningen, og det kan nemt reducere kontrollen til en slags alibiscanning. Det betyder, at der kan være stor forskel på den sikkerhed, PCI-scanningen skulle give – og som PCI Council har ønsket – og den sikkerhed, som virksomhederne reelt har opnået.

Den form for selvbetjening er en fremgangsmåde, man typisk ser hos de ASV'er, der primært konkurrerer på prisen, og det er en fremgangsmåde, vi hos FortConsult altid har været kritiske over for, og som vi derfor aldrig selv har praktiseret som ASV.

Vi har altid været fortalere for, at ASV'en skal være en aktiv del af processen. Derfor er vi også tilfredse med, at de nye regler i langt højere grad end de gamle regler tydeliggør, at ASV'en skal involveres i scanningsforløbet for i kundens egen interesse at kontrollere, at det reelle sikkerhedsniveau følger PCI-standarden.

Konsekvenserne af de nye regler

Som køber af en PCI-scanning vil de nye procedurer bl.a. medføre, at jeres ASV fremover skal kontrollere, at de informationer, I indtaster, er korrekte, at scanningen er foregået korrekt, og at scanningsrapporten er retvisende.

De nye regler påpeger desuden specifikt, at ASV'en altid skal dobbelttjekke scanningsresultater, som formodes at indeholde falske positive.

Virksomheden skal selv undersøge de formodede falske positive og forklare, hvorfor det blot er en fejl i scanningsmekanismen og ikke en reel sårbarhed. Det gælder også, hvis man får en falsk positiv to kvartaler i træk uden at have ændret på konfigurationen. Det vil naturligvis gøre processen mere krævende end tidligere,

og for mange vil det blive et irritationsmoment. Men ud fra et forsigtighedsprincip mener vi, at skærpelsen giver god mening, fordi noget, der ligner en falsk positiv, af og til faktisk viser sig at være en reel sårbarhed.

Mere fokus på webapplikationer

De nye regler betyder også, at webapplikationstesten er blevet opprioriteret, hvilket vi er særdeles tilfredse med. Området var næsten fuldstændig overset i de gamle regler, selvom de fleste indbrud sker via sårbarheder i webapplikationer. Der er dog stadig langt til en decideret webapplikationstest, men den type test bør virksomhederne også selv udføre i forbindelse med kapitel seks i PCI-standarden. I praksis er der dog mange mindre virksomheder, som ikke får udført kontrollerne under kapitel seks og derfor nøjes med PCI-scanningen (og det vil naturligvis gøre dem noncompliant, at de ikke udfører alle kontroller).

Derudover indeholder reglerne også hjælp til situationer, hvor man bruger IDS/IPS, har outsourcet dele af løsningerne og mange andre situationer, man som kunde kommer ud for i dagligdagen, og som tidligere har været uklart beskrevet.

De nye regler løfter sikkerhedsniveauet

De nye regler har været længe undervejs og er blevet grundigt bearbejdet af mange forskellige interessenter. Det har også været nødvendigt at gennemarbejde dem, da de grundlæggende bygger på en MasterCard-standard, der er næsten 10 år gammel, og som oprindeligt ikke var koblet sammen med PCI-standarden (der er baseret på Visa CISP-standarden).

De gamle PCI-scanninger har efter vores mening ikke givet nævneværdig sikkerhed for de virksomheder, der fik foretaget scanningerne. Men de har som nævnt stadig givet en sikkerhedsgodkendelse på papiret, og i mange mindre virksomheders tilfælde har PCI-scanningen været det eneste, som er blevet foretaget af en ekstern leverandør for at validere, om virksomheden overholder PCI-standarden.

Derfor er de nye procedurer efter FortConsults vurdering et skridt i retning af bedre sikkerhed, fordi de gamle regler ikke i tilstrækkeligt omfang har formået at sikre, at hensigten med PCI Councils regler blev understøttet. Derfor håber vi også, at formuleringerne i de nye regler er klare nok til at luge ud blandt ASV'er i branchen. Nogle ASV'er har nemlig hidtil udnyttet hullerne i det gamle regelsæt til at udbyde discountscanninger, som desværre har været med til at udvande kvaliteten af PCI-scanningerne. Dermed har de ASV'er også været med til at underminere både standarden og i sidste ende også sikkerheden hos kunderne.

De nye regler vil derfor formentlig betyde, at lavprisscanningerne stiger i pris – medmindre det lykkes lavpris-ASV'erne at finde en ny smutvej uden om PCI Councils regler og intentioner. Hos FortConsult forventer vi ikke, at vi ændrer prisen på ASV-scanninger, da vi hele tiden har været involveret i scanningsprocessen for at sikre, at vores kunders scanninger er blevet udført ud fra de korrekte procedurer.

Lige nu er det frivilligt for ASV'erne, om de vil følge de nye eller de gamle regler, men fra 1. september skal ASV'erne følge de nye regler.

4. De simple PCI-løsninger er tit bedst og billigst

Når vi holder indlæg på PCI-konferencer rundt omkring i verden, bliver vi bagefter ofte kontaktet af hardware- og softwareleverandører, der gerne vil have os til at kigge nærmere på deres PCI-sikkerhedsløsninger og anbefale dem til de kunder, vi er QSA (Qualified Security Assessor) for. Det skyldes, at mange af hardware- og softwareleverandørerne har set muligheder på PCI-området, og i mange tilfælde har QSA'ere også en ganske god forretning ud af at sælge løsninger ved siden af at udføre audits. Sammenblandingen af QSA- og leverandørrollen er imidlertid ikke uden problemer, fordi det skaber en tendens til, at kunderne ofte ender med at købe for komplicerede og for store PCI-løsninger, når man sammenligner med deres reelle behov.

Efter vores mening er det vigtigste for en QSA, at de bevarer uafhængigheden, så kunderne altid ved, at de kan stole på de råd, QSA'en giver dem om, hvad de skal ændre i deres sikkerhedssystem for at overholde PCI-standarden. Hvis man ligesom en mekaniker både påpeger problemet og sælger løsningen på samme problem, mister man en del af troværdigheden, og derfor takker vi som regel nej til at samarbejde med dem.

Mange virksomheder forkøber sig i PCI-løsninger

Som kunde hos en QSA er problemet tit, at man ikke altid er klar over, hvilken løsning der skal til for at overholde PCI-standarden. Derfor ser vi en tendens til, at mange virksomheder kommer til at forkøbe sig i alt for avancerede løsninger på PCI-området. Det skyldes både, at kunderne ikke altid selv har styr på, hvordan de opfylder et konkret krav i PCI-standarden, men også at mange kunder bliver overvældet af de mange funktioner, der typisk er i de store totalløsninger.

Problemet med mange af de avancerede løsninger er, at de bygger på standardsikkerhedsprodukter, der typisk ikke er designet til at imødekomme kravene i PCI-standarden, men som i stedet er lavet til at dække over mange forskellige typer af sikkerhedsbehov. Selvfølgelig kan mange af produkterne justeres, så de lige nøjagtig dækker et bestemt punkt i PCI-standarden, som fx overvågning af logfiler eller id-management. Men vi ser tit, at det kommer bag på en virksomhed, at den avancerede løsning, de har investeret i, faktisk ikke overholder alle PCI-reglerne, men skal suppleres med en eller flere andre løsninger. Det gør det tit svært for virksomhederne at overskue og administrere PCI-løsningerne, og så kan de nemt havne i en situation, hvor deres PCI-løsning aldrig bliver ordentligt implementeret. I mange tilfælde ser vi meget dyre og avancerede løsninger, som ikke er implementeret ordentligt i organisationen og derfor slet ikke fungerer efter hensigten.

Men det behøver faktisk slet ikke at være så svært.

Hjemmelavede løsninger rækker langt

Mange af vores kunder har udviklet deres egne løsninger, som er simple, og som virker rigtig godt. De bliver godkendt af os som QSA, og så er de desuden typisk meget velintegrerede i virksomhedens øvrige processer og eksisterende software.

Det gælder med andre ord om at finde en løsning, som opfylder de behov, man helt konkret har på PCI-området, og så sørge for at få den løsning implementeret i dagligdagen. Det giver nemlig oftest både den sikreste og billigste løsning og en proces, som gør det nemmest muligt at overholde PCI-standarden.

I næste nyhedsbrev kan du læse mere om den nye PCI-standard, der træder i kraft 1. januar 2011.

Med venlig hilsen

Lars Syberg
PCI Product Manager

FortConsult A/S

FORTCONSULT

Klar besked om it-sikkerhed

FortConsult Tel +45 7020 7525
Tranevej 16 - 18 Fax +45 7020 7526
DK-2400 Copenhagen NV www.fortconsult.net